TECHNICAL SPECIFICATION

ISO/IEC TS 19608

First edition
2018-10

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

Lignes directrices pour l'élaboration des exigences fonctionnelles de sécurité et de confidentialité fondées sur l'ISO/IEC 15408



Reference number
ISO/IEC TS 19608:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **2**
5 Purpose and structure of this document **2**
6 Requirement definition **3**
6.1 General 3
6.2 Security functional requirements (SFRs) 4
6.2.1 General 4
6.2.2 Example of security functional requirements 4
6.2.3 The selection, assignment, refinement and iteration operations 5
6.2.4 Dependencies between components 6
6.2.5 Structure of security functional components 6
6.2.6 List of classes 6
6.3 Procedure to specify security functional requirements 7
6.4 Procedure to develop functional components 8
6.4.1 Procedure 8
6.4.2 Existing components for privacy requirements in ISO/IEC 15408-2 8
6.4.3 Extended components for privacy requirements in published PP/STs and research papers 9
7 Privacy principles **9**
7.1 General 9
7.2 Input for extended components 9
7.3 Procedure to develop privacy requirements from privacy principles 10
7.4 Extended components for privacy 10
7.4.1 “Consent and choice” principle 10
7.4.2 "Purpose legitimacy and specification" principle 13
7.4.3 "Collection limitation" principle: Collecting PII 13
7.4.4 "Data minimization" and "Use, retention and disclosure limitation" principles 13
7.4.5 "Openness, transparency and notice" principle 17
7.4.6 "Individual participation and access" principle 18
7.4.7 "Accuracy and quality" principle 18
7.4.8 "Accountability" and "Privacy compliance" principles 19
7.4.9 "Information Security" principle 19
8 Summary of extended components and related privacy principles **20**
8.1 General 20
8.2 Extended components - general definition 20
8.2.1 General 20
8.2.2 "Consent and choice" principle 20
8.2.3 "Data minimization" and "Use, retention and disclosure limitation" principles 21
8.2.4 "Openness, transparency and notice" principle 22
8.2.5 "Individual participation and access" principle: Challenging the accuracy and completeness of PII 23
8.2.6 "Accuracy and quality" principle: Updating PII periodically 23
Annex A (informative) **Existing components used for privacy requirements** **25**
Annex B (informative) **Extended components for privacy in existing Protection Profiles** **32**
Annex C (normative) **Example of extended components for privacy** **36**

© ISO/IEC 2018 – All rights reserved

Bibliography **48**

 © ISO/IEC 2018 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2018 – All rights reserved

Introduction

ISO/IEC 29100 defines a framework of privacy principles that should be considered when developing systems or applications that deal with personally identifiable information (PII). This document analyses those principles and maps them, where possible, to the security functional requirements defined in ISO/IEC 15408-2. Where such a mapping is not possible, this document derives new security functional requirements collected in one new class that contains several families of privacy related security functional components following the guidance for developing new classes, families and components provided in ISO/IEC 15408-1 and ISO/IEC 15408-2.

This document can also be used as guidance for developing further privacy functional requirements using the framework of ISO/IEC 15408. The class, families, and components defined in this document can be extended for cases where the components defined here are not sufficient to express specific privacy functional requirements.

© ISO/IEC 2018 – All rights reserved

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

1 Scope

This document provides guidance for:

— selecting and specifying security functional requirements (SFRs) from ISO/IEC 15408-2 to protect Personally Identifiable Information (PII);

— the procedure to define both privacy and security functional requirements in a coordinated manner; and

— developing privacy functional requirements as extended components based on the privacy principles defined in ISO/IEC 29100 through the paradigm described in ISO/IEC 15408-2.

The intended audience for this document are:

— developers who implement products or systems that deal with PII and want to undergo a security evaluation of those products using ISO/IEC 15408. They will get guidance how to select security functional requirements for the Security Target of their product or system that map to the privacy principles defined in ISO/IEC 29100;

— authors of Protection Profiles that address the protection of PII; and

— evaluators that use ISO/IEC 15408 and ISO/IEC 18045 for a security evaluation.

This document is intended to be fully consistent with ISO/IEC 15408; however, in the event of any inconsistency between this document and ISO/IEC 15408, the latter, as a normative standard, takes precedence.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408 -1, ISO/IEC 18045, ISO/IEC 29100 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

© ISO/IEC 2018 – All rights reserved

— IEC Electropedia: available at https://www.electropedia.org/

3.1
privacy functional component
extended component that serves as a standard template on which to base *privacy functional requirements* (3.3) for TOEs

3.2
privacy requirement
requirement, stated in a standardized language, which is meant to contribute to achieving the technical privacy controls for a TOE based on *privacy functional requirements* (3.3)

3.3
privacy functional requirement
PFR
translation of the technical privacy controls for the TOE into a standardised language based on *privacy functional components* (3.1)

4 Symbols and abbreviated terms

The following abbreviated terms are used in this document.

MRTD	Machine Readable Travel Document
OSP	Organizational Security Policy
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PP	Protection Profile
SPD	Security problem definition
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TRA	Threat Risk Assessment
TSF	TOE Security Functionality

5 Purpose and structure of this document

Research shows that security and privacy should be considered from the beginning of the development life cycle for IT products, systems and applications in order to avoid expensive rework and reduce potential problems.

Security and privacy should also complement and mutually reinforce each other. The degree of protection should depend on the sensitivity of data and the linkability of data to personal identifiers. Therefore, successful implementation of security and privacy depends on defining accurate and complete requirements for both in a coordinated manner from the start of the development.

ISO/IEC 15408-2 defines a catalogue of security functional requirements (SFRs). ISO/IEC TR 15446 also provides detailed guidance on how to specify SFRs for a Target Of Evaluation (TOE). Developers can refer to these documents to specify SFRs to protect PII and other assets.

© ISO/IEC 2018 – All rights reserved